To Wield Excalibur: Seeking Unity of Effort in Joint Information Operations

CDR Synthia S. Jones, USN
Maj Bernard Flowers, USAF
Maj Karlton D. Johnson, USAF

Joint Forces Staff College
Joint and Combined Staff Officer School
Class 02-2I
7 June 2002

Faculty Advisor: Lt Col Bruce Reed
Seminar 06

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
07 JUN 2002	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
To Wield Excalibur: Seeking Unity of Effort in Joint Information Operations	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
CDR Synthia S. Jones, USN; Maj Bernard Flowers, USAF; Maj Karlton D. Johnson, USAF	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Joint Forces Staff College 7800 Hampton Blvd Norfolk, VA 23511-1701	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
Taken from the internet.

14. ABSTRACT
See report.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**26**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Table of Contents

I. Student Biographies

Commander Synthia S. Jones, USN is an Information Professional Officer who has held positions as: Head of Computer Operations Facility for the Navy Regional Data Automation Center; ADP Officer for the Bureau of Naval Personnel's Information and Personnel Security Directorate; Program Manager for Base Communications Office A-76 Studies at Naval Computer and Telecommunications Command and Executive Officer of Director, Communications Security Material Systems as well as Transient Personnel Unit Treasure Island. She has a Bachelors Degree in Mathematics and Masters Degrees in Information Technology Management and National Security and Strategic Studies. Upon completion of Joint Forces Staff College, she will report to the Applications Directorate of Defense Information Systems Agency in Arlington, VA.

Major Bernard Flowers is a USAF Communications and Information Officer. In nearly fifteen years of service, he has completed tours of duty at Williams AFB Arizona, Spangdahlem AB Germany, Schriever AFB Colorado, Ft. Belvoir Virginia and the Pentagon. He holds a Masters Degree in Public Administration and has specific experience in the fields of Satellite Communications, Acquisition Program Management and Communications and Information Plans and Policy. After graduation from Joint Forces Staff College, Major Flowers will report to his new assignment at the Joint Information Operations Center in San Antonio Texas, where he will serve as an Information Operations Staff Officer.

Major Karlton D. Johnson, USAF, is the Chief, Communications and Information Systems Plans Section, Supreme Headquarters Allied Powers Europe, Mons, Belgium. In this capacity, he leads, directs and provides consultancy on advanced information systems technology implementation and development activities for NATO, Allied Command Europe, and Partnership for Peace nations. He is also responsible for leading NATO and ACE Command and Control Working Groups, developing and executing knowledge management initiatives, and ensuring compliance with NATO Information Systems standards. Additionally, he develops communications requirements for ACE and subordinate command Combined Air Operations Centers, and provides oversight of the NATO Consultation, Command and Control Agency strategic plan.

II. Introduction

Throughout history, many authors have used European folklore as a medium to express complex ideas and clarify issues. Most known is the legend of King Arthur, a memorable story replete with rich allusions and profound metaphors. The Arthurian legend depicts Britain as a divided country: factional and disjointed with feudal entities fighting for control of the land. All seemed lost until the Lady of the Lake gave King Arthur the sword, *Excalibur*. Wielding this sword with vision, Arthur unified the people to bring order to a troubled land. There is a similar need for order leading to unity of effort in the realm of Joint Information Operations (JIO).

Current JIO cannot be effectively executed because Information Operations (IO) is a dynamic discipline that transcends the military community, permeates the national level, and thus makes the effort exponentially more complex. That complexity raises many questions and provides few answers. This analysis will bring several of those important questions to the surface, and will propose that the joint community adapt a new JIO construct; one that reflects the true nature of multidimensional IO and unifies both joint and national efforts to prosecute an effective JIO campaign. The research will show that current service *and* joint IO doctrine are incomplete in that they restrict the focus of IO. The argument will be made that much of the IO service doctrine remains in draft form, and where there is policy, it addresses only portions of the discipline. Further, an attempt is made to answer the question, "Why create a CINC-IO?" Lastly, this Joint Critical Analysis (JCA) argues that the IO discipline is a lacking arena. As such, it requires evolutionary thinking of what it means to be "joint" rather than continuing with traditional approaches to fill the gap. Using concepts and impressions from well-respected strategists, the intent is to propose a new construct that will overcome current JIO limitations and facilitate effective unity of effort. As the Lady of the Lake wished of Arthur, it is hoped that the joint community will use this new version of *Excalibur* to form a new "Round Table" that will aid in the defense our country from potential aggressors.

III. Are Joint Information Operations Effective?

"*Information systems must be protected from attack and new capabilities for effective information operations must be developed. The increasing dependence of advanced societies and military forces on information networks creates new vulnerabilities. Potential adversaries could exploit these vulnerabilities through their own computer network attacks. Closely coordinating U.S. offensive and defensive capabilities and effective integration of both with intelligence activities will be critical to protecting the current U.S. information advantage.*"

> Deputy Secretary of Defense Paul Wolfowitz, Tuesday, April 9, 2002 (Prepared Statement for the Senate Armed Services Committee Hearing On Military Transformation)

a. Perspectives of Current Service and Joint Doctrine. Are Joint Information Operations effective? Although the concept of IO has existed for centuries, it was not until the last few years that doctrine began to include multidimensional IO (e.g. it includes the *entire spectrum* of IO activities) at the joint level in any deliberate or systematic method. Additionally, the U.S. has not conducted a JIO campaign that included the entire cast of players required (e.g. private sector, Federal Government, etc.). Thus, a model does not exist that would allow for a respectable comparison. According to the Research Team's findings, JIO tends to center around five primary themes: Public Affairs (PA), Civil Affairs (CA), Psychological Operations (PSYOP), Operations Security (OPSEC) and Deception. For example, a look at history shows JIO used during numerous U.S. campaigns with Bosnia as the one most frequently cited. In his paper on U.S. Information Operations in Bosnia, Col Kenneth Allard highlights JIO in terms of using public and civil affairs to synchronize military and political efforts in peacekeeping missions.[1] In another example, a review of military history revealed that the invasion of Normandy relied heavily on joint OPSEC and PSYOP activities to deceive Hitler's forces. Both instances claim that JIO was successful in each engagement, but does this mean that the joint community has a firm grasp of the concept of JIO? Alternatively, does it really mean that *portions* of the joint community are adept at using *portions* of the JIO discipline? The evidence points to the latter.

Consider, for example, the significant legal component of JIO that is critical to its effective use. According to the Department of Defense (DoD) Office of General Counsel, "the United States is a party to a variety of bilateral and multilateral agreements containing obligations that may affect information operations". [2] A review of *Joint Publication 3-13: Joint Information Operation* revealed that it includes a provision for addressing legal challenges by stating, "IO may involve complex legal issues requiring careful review and national-level coordination" and "IO planners should understand

---

[1] Col Kenneth Allard, "*Information Operations in Bosnia: A Preliminary Assessment*", NDU Strategic Forum, #91, Nov 1996, http://www.ndu.edu/inss/strforum/forum91.html

the limitations that may be placed on IO across the range of military operations".[3] However, beyond these statements, there is little available to help joint planners maneuver through the legal maze, and even less training available to facilitate this IO effort. This raises the perception that the joint community does not exercise this vital segment of the IO process. In fact, many engagements where JIO has been used were exercises in piecemeal implementation. U.S. Law either prohibits other facets of IO such as Computer Network Attack and Perception Management or they are practiced in limited fashion. Thus, important capabilities remain unexploited. How well then does the joint community perform those activities? The answer lies in an exploration of how specific services manage IO internally.

The services have either established IO doctrine or have a document in draft. A comparison of the service doctrine against Joint Publication 3-13 showed that each tended to view IO in terms of its own military doctrine. According to FM-100-6, Army Information Operations, the Army viewed IO from a "land-based operations" perspective (e.g. seeking information dominance to gain tactical advantage via digitization of the battlefield). The Navy's doctrine, NDP 3-13, is in development. Its closest sister, NDP 6, viewed IO in terms of Command and Control Warfare (C2W) for fleet operations. The Marine Corp IO doctrine also remains in development. Even the Air Force, while having a better view, focused on IO with respect to "air mindedness" and used it to control the dimensions of air and space. The question remains, "What does this review of service IO doctrine reveal?" It identifies that the services view IO in terms they can understand, thus keeping them along the comfortable path of the familiar. These findings were consistent with those of Randall C. Lane in his article "*Information Operations: A Joint Perspective*".[4] Lane presented a case study of how the services' varying approaches to IO fell short of an integrated joint approach. Is there a reason for this lack of integration? One is found in the Air War College article, "*The Search for a Science of Strategy: a Review Essay*" by Stephen M. Walt, where he references a concept called "the politicization of strategy"[5]. Although written in 1987, the article makes a salient point that is still true today. Walt noted that strategists charged with developing strategic ideas within the individual services are rarely "objective" scholars; their job is to ensure that their service's interests are promoted. This phenomenon is evident when considering the development of both service and joint IO Doctrine. In taking into account "the politicization of *doctrine*", one can see that each service is an expert within its

---

[2] Department of Defense, "*An Assessment of International Legal Issues in Information Operations*", Nov 1999
[3] Joint Publication 3-13, *Joint Doctrine for Information Operations, Oct 1998 (http://* www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf
[4] Randall C. Lane, "*Information Operations: A Joint Perspective*", Army School of Advanced Military Studies, may 1998

domain as dictated by law, and each one views doctrine via its respective "world view". The unfortunate side effect is that they apply the same principles used in their military doctrine to their IO doctrine. The problem with this approach is that the concept of IO transcends the traditional boundaries of modern warfare, and it should be engaged from an entirely different plateau. In essence, when thinking about JIO, one must get out of a "playing checkers" mindset and jump into a "three-dimensional chess" mode.

b. Who is in Charge of Information Operations? The tribulations associated with the effective application of JIO compound when one considers the challenges of coordinating IO-centric activities. Within the military, USSPACECOM wields responsibility for Computer Network Operations since the preponderance of space-based and computer-centric systems reside within its scope. They are also responsible for the Joint Information Operations Center at Lackland AFB, Texas. However, it would be inappropriate to call CINC-USSPACECOM the "CINC IO". This raises a very critical question: Who is in charge of JIO?

Consider the following fictional scenario. During OPERATION ANACONDA, USCENTCOM's command and control system is the recipient of a computer network attack. Simultaneously, al-Qaeda terrorists launch both a cyber attack and a perception management campaign on NATO websites to influence partner nations that it would not be in their best interest to support the U.S. anti-terrorism efforts. This second assault falls into the domain of EUCOM/SACEUR. A scenario like this raises several key questions. What is the new theater of operations for JIO or counter-JIO missions? How do we now define the battle zones and boundaries? What is the process for reciprocity on both attacks? Who is the main entity responsible for coordinating the response? These questions expose a clear gap in the JIO C2 process.

How does the combatant commander resolve the gap? Some say that we need a Combatant Commander to control the IO process. For example, Commander Robert J. Gaines, in his paper "*Future Information Operations in the Military – Is It Time for a CINC-IO*?"[6], postulates that the time is ripe for this type of Combatant Commander. He reasons that only a Unified Command responsible for IO could provide the vision, focus and span of control necessary to protect national infrastructures from enemy IO aggression. CDR Gaines is not alone in this belief. Lieutenant Commander William J. Jensen proposed similar courses of action in his paper "*Information Warfare's Missing Quarterback –*

---

[5] Stephen M. Walt, "*The Search for A Science of Strategy: A Review Essay*,"(**International Security**, Vol.12, No. 1, Summer 1987, pp. 140-160)

The Case for a Joint Information Warfare Component Commander". [7] LCDR Jensen's viewpoint is that a Joint Forces IW Component Commander is needed to resolve IO planning problems and enable the successful execution of multifaceted IO missions. These are sound arguments, and they are close to the answer. However, a CINC-IO is not enough. Today's threats and the ubiquity of information technology have dramatically changed the boundaries of IO. Although the Combatant Commanders will play a critical role in IO campaigns, a single CINC-IO would not have the resources, competencies, or partnerships necessary to handle the enormity of the tasks. In fact, a CINC-IO could have the opposite effect. If the community holds one Combatant Commander responsible for JIO, the others may choose to "punt" their IO problems to that Combatant Commander rather than collaborating for success. Possible turf wars could erupt if funding becomes associated with the positions (which is likely). In short, a single CINC-IO could marginalize the effort and diminish its importance in military operations planning. Every Combatant Commander needs to have a play in the JIO process. However, they are not the only critical players in this game.

c. National Complexities and Implications of IO. The inclusion of national, governmental and private sector entities in the equation further complicates IO. Realistically, if the United States suffers an IO attack, it will not necessarily be limited to military elements. As identified in Presidential Decision Directive 63, the U.S.' national infrastructure is a prime target for hostile powers.[8] Moreover, the "9/11" attacks proved that the minds of the American public are a key target for IO assaults. Consider the crash of the first plane into the World Trade Center. Few people saw the initial impact, and fewer still captured it on camera or videotape. *Nearly every newsroom in the world was tuned in when the second terrorist event sent the crystal clear the message "You Are Not Safe".* Consider the tremendous IO impacts of the attacks for a moment, specifically the perception management aspect. The enemy "psychological attack" had significant results: The airline industry nearly went under, stocks plummeted, and *Americans were <u>scared</u> within the confines of <u>their own homes</u>*. It is unclear whether the U.S. realized, at that moment or before, the IO impact of the second attack. Also unclear were the possible countermeasures the U.S. could have or *should have* employed to minimize the power of the event. The facts indicate there should have been significant collaboration of effort between government, private sector, military, and media elements to combat the IO attack.

---

[6] CDR Robert F. Gaines, "*Future Information Operations in the Military – Is It Time for a CINC IO*?", Air Command and Staff College, Apr 2000

[7] LT CDR William J. Jensen, "*Information Warfare's Missing Quarterback – The Case for a Joint Force Information Warfare Component Commander*", Naval War College, Feb 1998

[8] Presidential Decision Document 63, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

However, this did not occur. In truth, the U.S. seemingly has little in the way of tactics, techniques, procedures (TTP) or processes to harmonize the complex efforts of these actors and to combat asymmetric IO attacks of this magnitude. As noted in a Joint Forces Staff College paper by Lieutenant Colonel Henry Huntly, Maj Michael Yaguchi, and Lieutenant Commander Michael Goshgarian, both *Joint Vision 2020* and Joint Publication 3-61 (PA) encourage the JFC's use of the media to shape the battlespace,[9] but what relationships and TTPs have been formed? These issues compounded with the legal concerns and American distrust of IO (as seen with the demise of the Office of Strategic Influence) makes the joint community's job even more complex.

d."Painting Over the Old Lance" - Laying a New Concept on an Old Template. What has been the U.S. response to these JIO issues? Unfortunately, the reply has been to "paint over the old lance". From a joint perspective, military leaders recognize that JIO is critical to future engagements. These leaders have made their best attempt to forge joint doctrine into something viable. Even so, something entirely different happened. The doctrine drafters took traditional ways of fighting and applied those historical concepts to new the JIO strategy. Based on the evidence, one can clearly see that this has not been the most effective approach. "Tried and true" battle strategies will not win future wars fought in the continuum between the human mind and the ephemeral cyberspace. Contemplate the fact that the battlefield itself has changed on a moral, physical, and cybernetic level.[10] Additionally, tools and technologies have radically changed, decreasing the battle rhythm to seconds instead of days, thus enabling a level of influence unseen before in human history. The so-called "CNN Effect" is a clear representation of this fact. Therefore, one cannot afford to think and respond in old ways. Do we need a change? In a paper for the Center of Defense Information, Thomas B. Baines proposes the need for a paradigm that can guide the initiation and management of perception in synchronization with the initiation and management of actions to confront a "fractal battlespace". [11] This lends credence to the idea that joint warriors have to think *differently* about battlefields, TTPs, relationships, and even the actors in a new kind of war.

---

[9] Lieutenant Colonel Henry Huntly, Maj Michael Yaguchi, and Lieutenant Commander Michael Goshgarian, "*Another Battlefield Domain? How the Media Impacts Joint Operations*", JFSC Paper, Sep 2000

[10] Lt Col Tom Jukes, "*Battlespace Management*" (PowerPoint), Joint Forces Staff College / NDU seminar presentation, May 2002

IV. Seeking Excalibur to Heal the Land – Changing the Situation

"!Mira! Mira! Llega la tormenta!" "What did he say?" asked Sarah Connor." He said, 'A storm is coming", replied the Attendant. Sarah gazes at the thunderheads building up out over the desert. Sadly, quietly, she responds, "I know."

Excerpt from The Terminator

There IS a storm coming. The events of 11 September 2002 were just the heralds of it. In truth, the joint team is not prepared for the magnitude of its passing. Take into account the following cases:

- The Terrorism Research Center maintains an information database on cyber attacks against the U.S. This database reflects an alarming increase in attacks originating from within other countries, and some of these are "friendly nations". [12]

- Congressional testimony by the Central Intelligence Agency's IO Issues Manager, John Serabian, reported that the U.S. is increasingly vulnerable to cyber attacks by an increasing list of terrorist and foreign governments.[13] Serabian explained that said countries are using IO to "level the playing field" when engaging the U.S. In effect, IO serves them as a "David" to the U.S.'s "Goliath".

- In their book "Unrestricted Warfare", Chinese Colonels Qiao Liang and Wang Xiangsui advocate the use of new Information Operations methods to change the concept of war as "Americans are inadequately prepared" to deal with these new threats. [14]

- In further testimony to the U.S. Senate, Mr. James Adams, CEO, Infrastructure Defense, Inc., stated that over "30 countries have aggressive offensive IW programs and all of them have America firmly in their sights." [15]

Slowly, quietly, hostile forces are encircling the U.S. If it is to survive the threat, the U.S. must change the ways in which it thinks about and plans for Information Operations events. One can begin by taking lessons from the legend of King Arthur.

---

[11] Thomas Baines, "*Military Information Operations: An Unifying Paradigm*", A Paper for the Center of Defense Information

[12] Cited from the Terrorism Research Center, http://www.terrorism.com/iwdb

[13] "*CIA: China, Russia Develop Cyber Attack Capability*", Jack McCarthy, IDG News Service, Feb 2000

[14] Colonels Qiao Liang and Wang Xiangsui, "Unrestricted Warfare", Beijing: PLA Literature and Arts Publishing House, Feb 1999, http://www.terrorism.com/documents/unrestricted.pdf

[15] Testimony of James Adams, CEO, Infrastructure Defense Inc., Committee on Governmental Affairs, U.S. Senate, Mar 2000

a. Forming the Round Table: Service to Joint Team Unity of Effort. According to legend, King Arthur realized the need to bring the people together and save Britain. He created the "Round Table" to serve as a forum for Knights to join in equal stature and talk of deeds brave and noble. The Knights of the 21st Century need a similar forum, but one that will allow them to do more than just talk. Figure 1: Harmonizing Service IO Functions reflects the composition of that team.

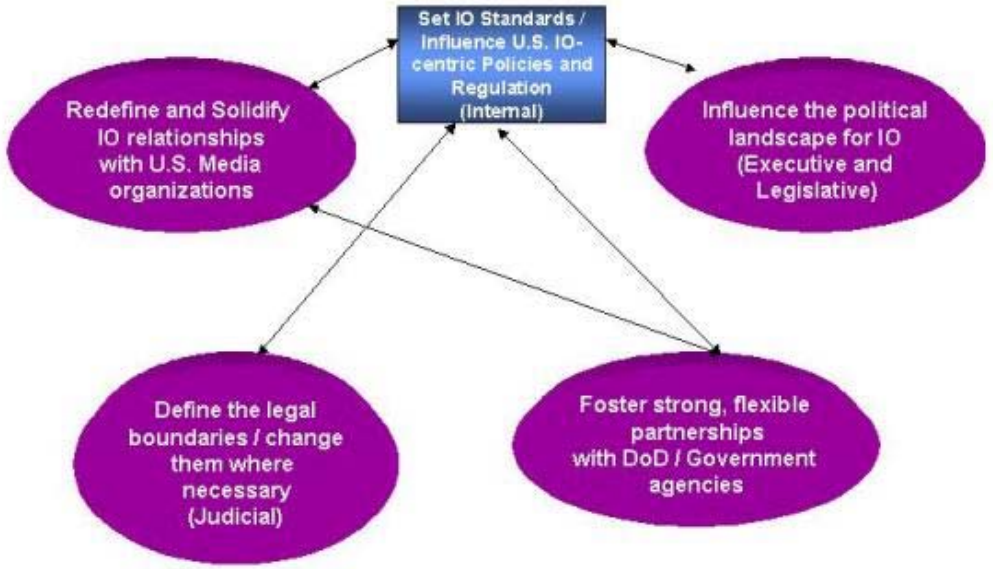
Figure 1: Harmonizing Service IO Functions

In this figure, the Combatant Commanders provide a representative at the table. As was noted, each service retains its own IO doctrine created based on its operational "world view". Effective change will commence once service doctrine evolves to transcend the boundaries of service "group think", and begins to disassociate IO from service-specific control. Joint leadership must work together to help break down the parochial walls and guide their services towards a purer form of JIO. The current version of JP 3-13 is a good start for this as it outlines a decent IO template. However, it falls short by being conceptual rather than directive in telling services the forms a synchronized JIO effort would take. This is a fine line. Should the JCS guidance be directive down to the service level? As it could infringe

on Combatant Commander authority, this would be a valid concern. Nevertheless, there has to be a better way to leverage service competencies in this regard. The Combatant Commanders remain the key to success at this level, and they must guide their teams to break down service-centric barriers and develop a process more applicable for the times.

b. Expanding the Round Table: Rethinking "DoD Jointness" and "National Jointness".

Figure 2: Setting IO Standards and Building Key Relationships



In parallel with the Combatant Commanders' efforts, the joint IO community should expand the "Round Table" outward to include other entities critical for effective IO campaigns. If the worst-case scenario happens, the U.S. military will not be the only team to engage and defend against the enemy. It will need significant assistance from agencies within the government such as the National Security Agency (NSA), Central Intelligence Agency (CIA), and National Imaging and Mapping Agency (NIMA) to facilitate IO initiatives. Effective JIO will *also* require strong partnerships with the judicial arm of government to ensure the actions taken are legal and will withstand the "Washington Post" test if

revealed for world judgment. Linkages with national media will be an absolute necessity to ensure the truth gets to the American and global public when the U.S. engages in or responds to IO. Figure 2: Setting IO Standards and Building Key Relationships reflects the types of relationships needed to make this work. By leveraging these relationships effectively, the joint team will be able to design cross-functional responses for IO, and thus have a hand in influencing the entire landscape of IO. These new partnerships take on a more realistic shape for "jointness"; they change the size of the joint team to include all affected stakeholders and allow us to leverage our full national capacity against the threat.

c. *Wielding Excalibur: Uniting the Effort with a New Construct for "Joint Information Operations"*

"Strategists cannot afford to look at the world from one point of view. Doing so is as dangerous as trying to navigate the freeway with one eye closed. Instead, we need a comprehensive framework that uses a variety of lenses and tools to understand our world (IO) situation, find new sources of advantage, and formulate strategies that our enemies are unable to match readily."

(Adapted from Wharton on Competitive Strategy)

Everything written up to this point has been driving towards a single thought: The U.S. needs unity of effort for JIO. The old models no longer work, and the joint community needs to think differently about the problem to obtain a workable solution. Dr. Daniel Kuehl, one of the most respected experts in the IO discipline, agrees. He wrote,

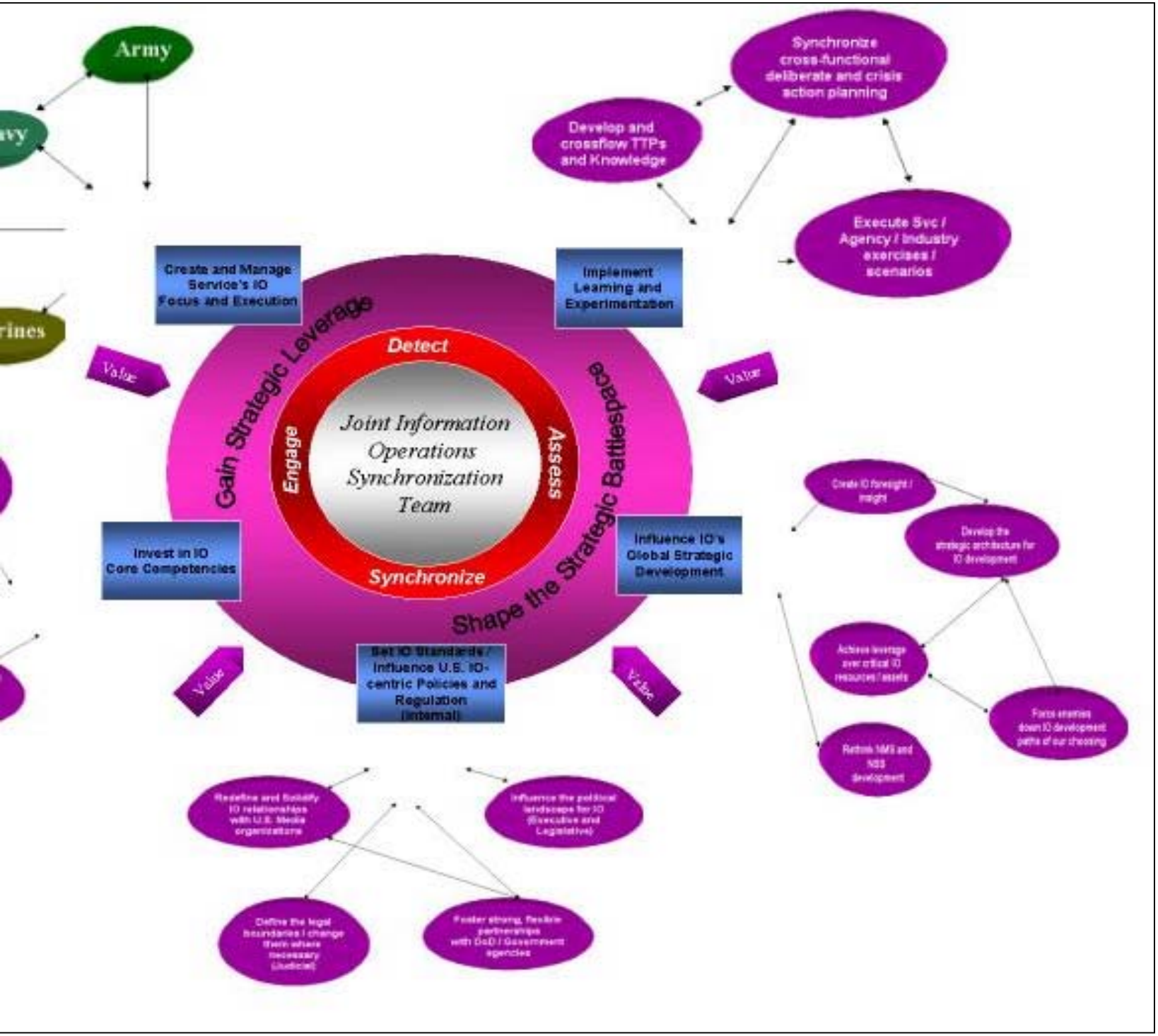
> "The impacts and implications of the information revolution are so widespread that they necessitate a broader, more inclusive concept incorporating all of the various elements of national information power. National security in the information age and the development and exercise of the information component of national power requires a new paradigm of jointness that incorporates and synchronizes the policies and activities of all the players in the information realm." [16]

Others have also advocated the need for harmonization and stronger unity of effort. In James Adams's testimony to the Senate, he references the need to "leave the old body [and] move into a new one" by "beginning to make changes in our cultural, political, and economic processes and institutions of such

[16] Dr. Dan Kuehl, "*Joint Information Warfare: An Information-Age Paradigm for Jointness*", NDU Strategic Forum, #105, Mar 1997 (http://www.defencejournal.com/march98/jointinfo.htm

magnitude that they will dwarf even those that accompanied the industrial revolution". [17] There is wisdom in the words of Dr. Kuehl and Mr. Adams. Thus, a new version of *Excalibur* is offered to solidify unity of effort in Joint Information Operations.

[17] Ibid – James Adams Testimony to the U.S. Senate


Army
Synchronize cross-functional deliberate and crisis action planning
Develop and crossflow TTPs and Knowledge
Execute Svc / Agency / Industry exercises / scenarios
Create and Manage Service's IO Focus and Execution
Implement Learning and Experimentation
Detect
Gain Strategic Leverage
Shape the Strategic Battlespace
Engage
Assess
Synchronize
Joint Information Operations Synchronization Team
Value
Value
Invest in IO Core Competencies
Influence IO's Global Strategic Development
Set IO Standards / Influence U.S. IO-centric Policies and Regulation (internal)
Value
Value
Create IO foresight / insight
Develop the strategic architecture for IO development
Achieve leverage over critical IO resources / assets
Force enemies down IO development paths of our choosing
Refine M&S and NSS development
Redefine and fortify IO relationships with U.S. Media organizations
Influence the political landscape for IO (Executive and Legislative)
Define the legal boundaries / change them where necessary (Judicial)
Foster strong, flexible partnerships with DoD / Government agencies

o

In addition to the plethora of doctrinal guidance, research papers, and articles available on the topic of JIO, the Research Team analyzed some of the best practices and thoughts from universities, consulting firms, and strategy experts to help forge an appropriate construct. Figure 3 depicts the results of those efforts. It relies heavily on the works of Gary Hamel, Professor of Strategic and International Management at London Business School, and C.K. Prahalad, the Harvey C. Fruehauf Professor of Business Administration and Professor of Corporate Strategy / International Business at the University of Michigan. In 1994, they co-authored a book called "Competing for the Future" in which they introduce the concepts of strategic intent, strategic architecture, and core competence. Their work redefined what it meant to be strategically successful by emphasizing an organization's need to "shape the future" rather than "respond to the future".[18] To do this means to foster a revolution in the field of expertise, and that is the crux what needs to happen concerning JIO. Additional sources used to construct the model were synthesized from the Wharton School of Business (Strategic Management) and the collected works of over 20 experts on strategy as found in the Portable MBA in Strategy.

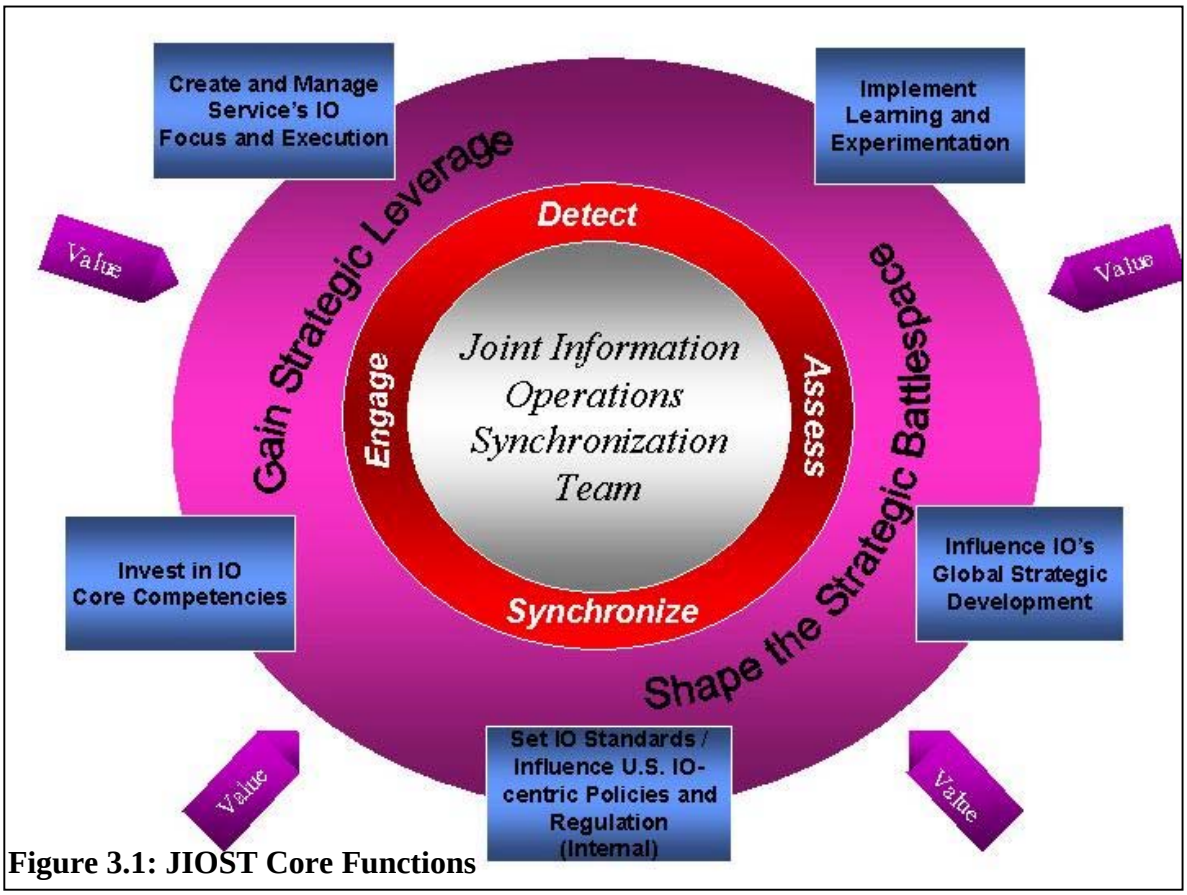


Figure 3.1: JIOST Core Functions

[18] Gary Hamel and C.K. Prahalad, "Competing for the Future", Harvard Business School Press (1994)

The heart of this construct revolves around the formation of a true "Joint Information Operations Synchronization Team (JIOST)" (See Figure 3.1). It is comprised of members from five communities: the military (with members representing the Combatant Commanders), the Federal government (e.g. CIA, NSA, etc.), the Legislative / Judicial teams, key civilian industry leaders, and key media representative. Appointed by the SECDEF and led by the CJCS, these players form the "New Round Table", and they have the power to influence or accomplish the five facets of this construct. The JIOST will serve as a "full-spectrum fusion center" enabled to float between the operational and strategic levels of JIO. Their charter will be to "shape the future" of JIO through the acquisition and exploitation of competitive advantage. Part of their role will be to facilitate defensive IO efforts for the new joint community (e.g. *Detect* IO attacks against the U.S., *Assess* their impact, *Synchronize* the joint response, and *Engage* the teams to action [DASE]). However, the DASE function only represents the "We've been hit! What do we do now?" end of the business. The strength of the JIOST lies in its continued efforts to shape the strategic IO battlespace. The Joint Information Operations Center (JIOC) in Texas would serves as the interface to the services, but the JIOST would develop gateways to the rest of the team.

The construct has five components. Two of the five facets (shown in Figures 1 and 2) have been discussed already. The following three are key for reshaping the landscape of JIO.

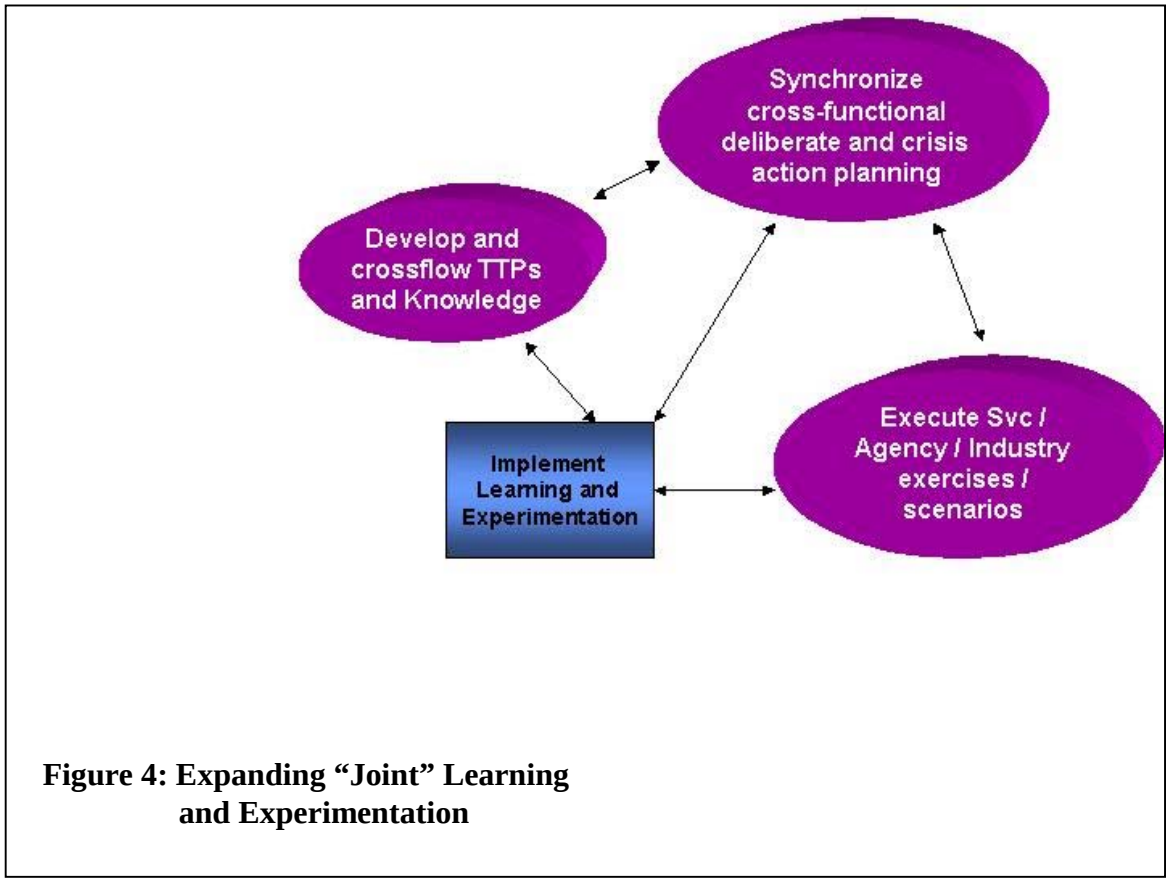


Figure 4: Expanding "Joint" Learning and Experimentation

Implement Learning and Experimentation: Current joint doctrine does provide for service-DoD/government exercises. However, those plans do not include key industry players in the scenarios. TTPs, knowledge assets, and plans are not shared with industry or with Media presidents such as CNN. The old adage of "train as we fight" is applicable to this situation. Figure 4: Expanding "Joint" Learning and Experimentation articulates the idea that all players must be included in the deliberate and crisis action planning process (*with the appropriate considerations made for security and protection of sensitive information*) to properly synchronize efforts in the event of an attack. Exercises should be planned and executed jointly; lessons and successes should be shared. As teams begin to form the necessary relationships (as stated in "Setting IO Standards / Influencing Policies"), lines of communication will open and the U.S. can begin to shape the future in earnest. The knowledge gained will prove invaluable towards the identification of vulnerabilities across the board: Technology, Partnerships, Competencies, etc. Formation of the needed relationships will prove to be the most daunting tasks in this process.

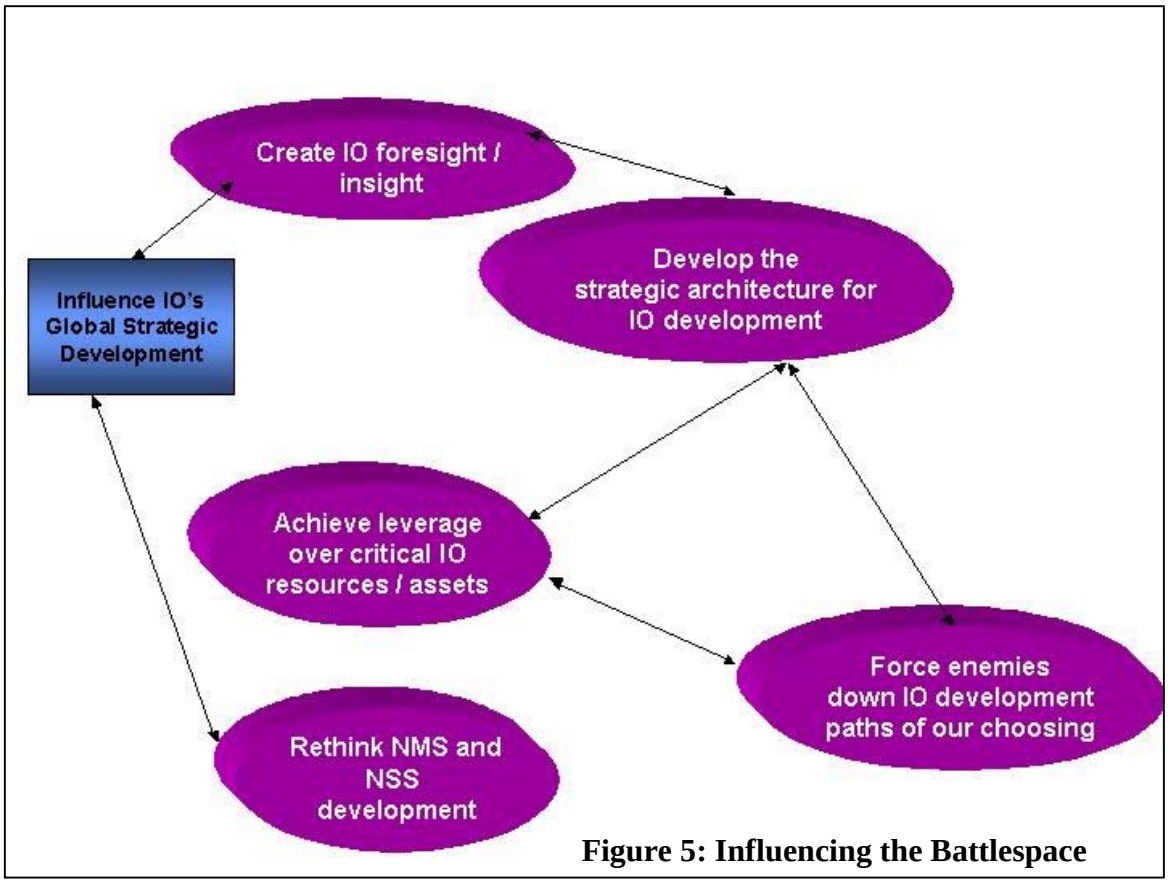


Figure 5: Influencing the Battlespace

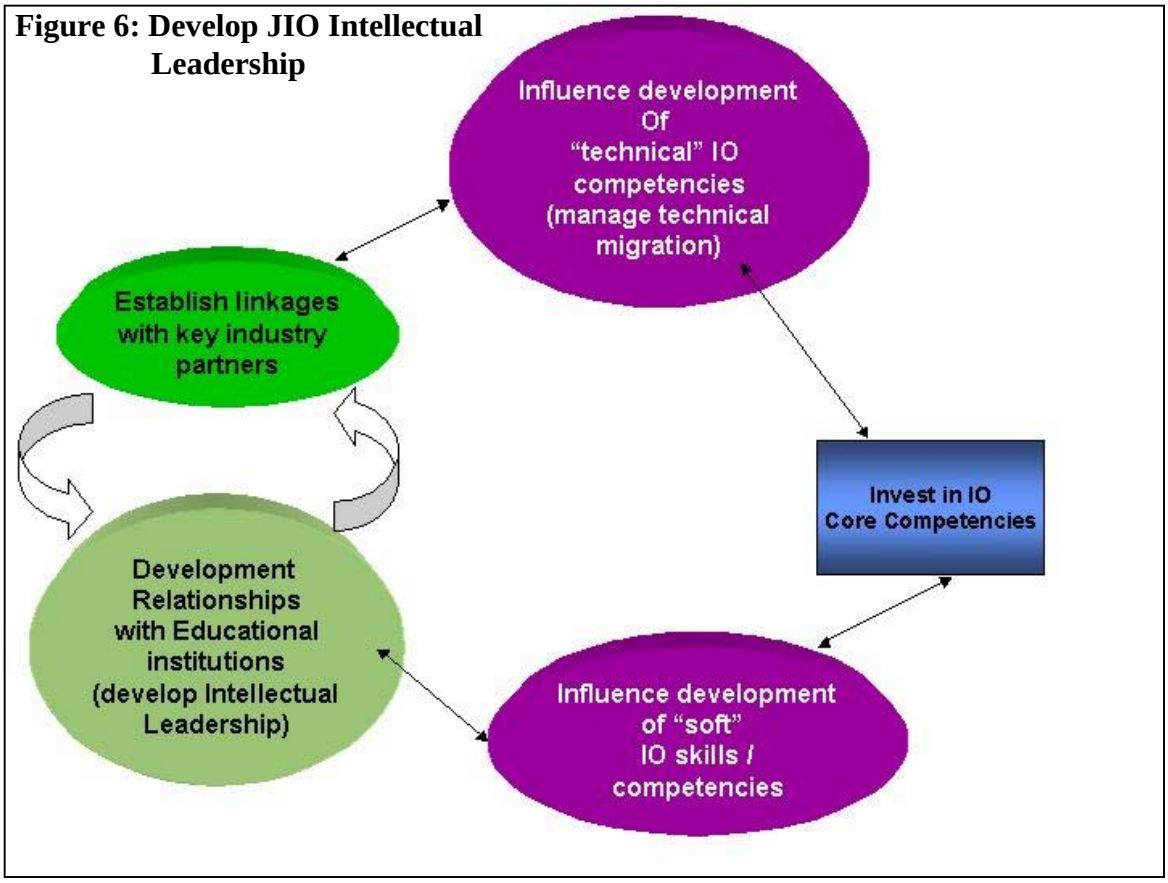
Influence IO's Global Strategic Development: Sun Tzu once wrote that it is the apex of strategy to win a fight without fighting. [19] The experts have already highlighted the various cases where other nations

[19] Sun Tzu, "The Art of War", Online Version, http://www.sonshi.com/learn.html

are training and planning IO initiatives to use against the U.S. Responding to the threat by *reacting* to it is a sure path to failure. Instead, the joint team needs to reshape the future to one of its choosing and force enemies into the "killbox" designated by it. By shaping the future of JIO, the U.S. gets to that future first and can force enemies to "bring a knife to a .50 cal fight". As shown in Figure 5: Influencing the Strategic Battlespace, the JIOST is the focal point for synergizing the effort. It is their charge to develop the strategic foresight into how IO should change over time, to synchronize the community's efforts for mapping a *strategic architecture,* and then to help "build" that future. According to Hamel and Prahalad, a strategic architecture is a "high-level blueprint for the deployment of new functionalities, the acquisition of new competencies (or migration of existing competencies), and the reconfiguring of the interface for those who receive the benefit of said competencies". [20]The JIOST would use this blueprint to forge a future where the U.S. influences how other countries build IO TTPs. Since the U.S. has the best technology infrastructure in the world, it currently has leverage over how others could use technology and IO concepts. However, this lead is quickly diminishing. For example, during the Gulf War, Iraq was able to effectively use IO as an asymmetric tool. With it, they were able to influence international opinion and thus affect U.S. policy.[21] Clearly, a race is on. This means that the U.S. cannot afford to sit back and watch. It needs to set the pace and establish the standard. It also means that the U.S. needs to rethink how it develops the National Security Strategy and the National Military Strategy. In "Unrestricted Warfare", Liang and Xiangsui cited their extensive use of U.S. doctrine and guidance to formulate their conclusions. [22] The U.S. can use documents like these to guide the rest of the world down the road we want them to walk while simultaneously forging ahead on a different vector. Since Perception Management is a critical component of IO, the U.S. should become experts in global Perception Management. The JIOST can aid in that endeavor.

[20] Ibid. Hamel and Prahalad, "Competing for the Future"
[21] From LTC(P) Ronald M. Bouchard, "*Information Operations in Iraq*", Strategy Research Project, U.S. Army War College, 1999
[22] Ibid. "Unrestricted Warfare", http://www.terrorism.com/documents/unrestricted.pdf

Figure 6: Develop JIO Intellectual Leadership



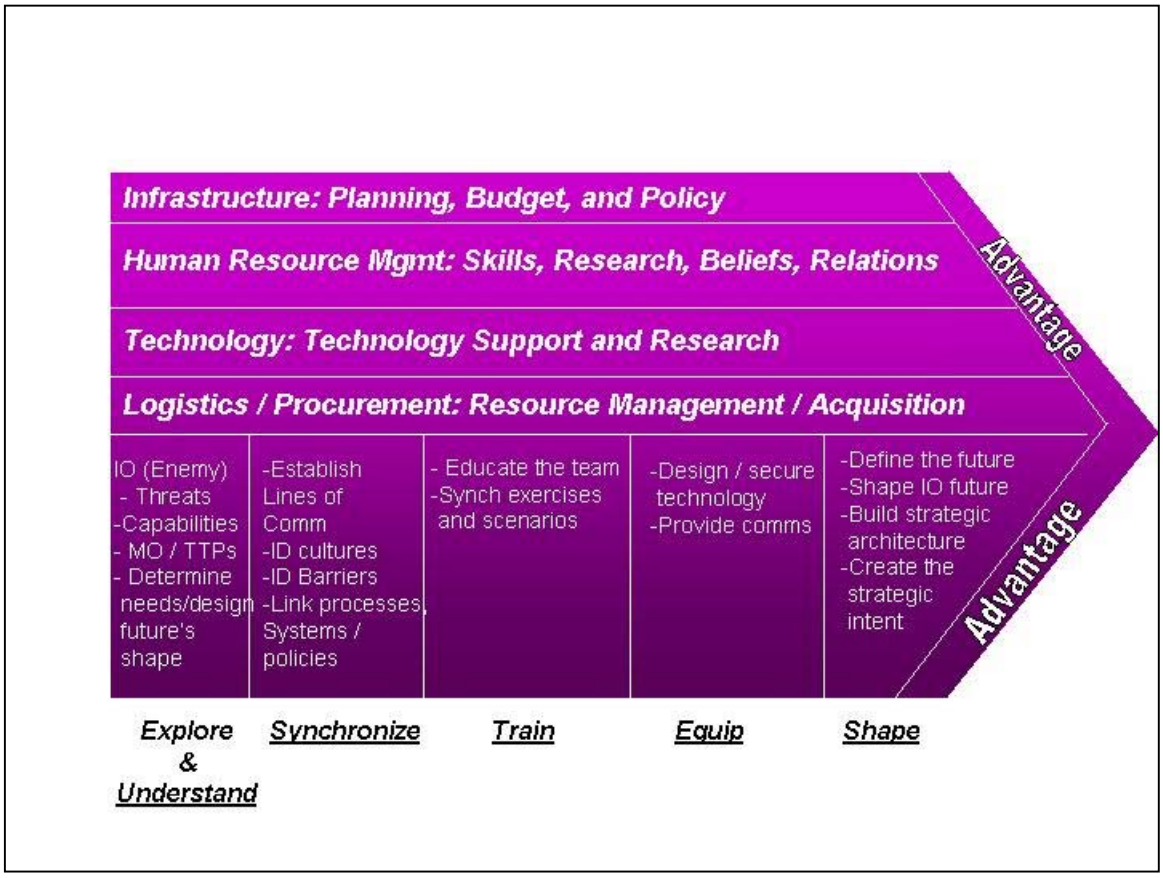
Invest in IO Core Competencies: The other side of shaping the battlespace involves the acquisition of the right bundle of skills and technologies that enables the U.S. to field a solid IO capability. Look at Figure 6: Develop JIO Intellectual Leadership. It shows that the JIOST would be responsible for setting the *Strategic Intent* of our IO efforts. Strategic Intent implies a particular point of view about the long-term environment in which an organization hopes to build a competitive position over time.[23] Consider Strategic Architecture to be the "brain" and strategic intent to be the "heart" of the effort that implies significant stretch for the joint team. This intent would then translate into a discussion between the JIOST, learning institutions and technology-centric firms to determine what core competencies the U.S. would need in the future. Then, they would help to shape the development of those competencies, matching them to the strategic architecture previously discussed. The result would be a joint effort to secure "intellectual IO leadership", influence the strategic landscape of the battlespace and preempt any advantages of possible use to potential enemies.

The Joint Information Operations Value Chain: Clearly, the path to effective JIO lies through achieving unity of effort by redefining how the U.S. views "jointness" and rethinking the processes for

[23] Ibid, "Competing for the Future"

shaping the strategic battlespace. Each step in this construct attempts to add layers of improved value into the process, and this new value takes the JIOST to even higher levels of possible accomplishment. Based on the work of consultants at McKinsey and Company in Boston and Michael Porter, a well-known expert of strategic management and business strategy, [24] the Research Team constructed the JIO Value Chain below.

Table 1: Joint Information Operations Value Chain



The JIOST consists of several moving parts that affect critical areas: Infrastructure, Human Resource Management, Technology, Logistics, etc. Those areas must be harmonized to produce some value that facilitates the effective employment of JIO and gains a competitive advantage in this discipline for the U.S. As the JIOST works through the JIO construct, it would be mindful of the need to establish a competitive advantage and continually strive for enhanced value in every activity. The JIO value Chain serves as a visual queue for asking and answering the question: How does this action create more value

[24] Michael Porter, "Competitive Advantage - Creating and Sustaining Superior Performance", The Free Press (1985) [Differentiation and the Technology Value Chain Model, and Achieving Relationships], and Michael Porter, "Competitive Strategy - Techniques for Analyzing Industries and Competitors", The Free Press (1980). McKinsey and Company developed the Value Chain Model, and Dr. Porter has written several seminal articles / books on its effective use.

for the U.S., and does that value exceed the real or implied costs of producing it? This aspect of the construct is what separates it from other IO constructs produced by others.

V. Conclusion

This is not an easy subject to address. There are probably as many options, thoughts, and beliefs on the concept of Joint Information Operations as there are definitions in Webster's Dictionary. There are also equal amounts of unanswered questions concerning JIO. Despite those concerns, there are some very evident truths:

1) Information Operations will be both a strategic asset and a strategic liability for the U.S. in the coming years.

2) The U.S. can achieve a strategic, competitive advantage in this area if it chooses to shape the future rather than react to the future.

3) The U.S.' ability to shape the future will be achieved only when it has expanded its views on "jointness" to include the larger communities of industry and federal government, and together work towards defining the core competencies needed to prosecute effective Joint Information Operations campaigns.

Change sometimes requires "thinking out of the box". *Effective* change requires one to shred the old box up and elevate one's thinking. Using this new version of *Excalibur* as a construct for uniting U.S. JIO activities can help simulate thought and discussion so policy makers can attack the problem more effectively. By making the complex issues more understandable, it provides a framework for resolving many of the questions posed in this Joint Critical Analysis. Additionally, if followed to its logical conclusion, the construct can address the joint and interagency IO collaboration issues that remain some of the most prevalent challenges in this discipline. In reference to a previous analogy, it is time for the team to remove the checkers board in preparation for the 3-D chess game. It is time to Wield Excalibur and Seek Unity of Effort in Joint Information Operations.

VI. Bibliography

1. Abe Singer and Scott Rowell, "*Information Warfare: An Old Operational Concept with New Implications*", NDU Strategic Forum, #99, Dec 1996

2. AFDD 2-5, *Information Operations (Air Force Doctrine Document 2-5), 5 Aug 1998*

3. Briefing, "*Information Operations: Strategic Enabler for JV2020"*, Presented by the Joint Forces Staff College/Joint Information Warfare Division

4. Briefing: "*Block II – Intelligence and Exploitation*", Presented by the Joint Forces Staff College/Intelligence, Surveillance, and Reconnaissance Focus Study Team

5. CDR Robert F. Gaines, "*Future Information Operations in the Military – Is It Time for a CINC IO?*", Air Command and Staff College, Apr 2000

6. CDR Sandra Lawrence, Maj Joe Adams, and Maj Jay Bruhl, "*Organizing for Success: A New Paradigm for Information Operations*", Armed Forces Staff College Paper, Jun 2000

7. Christopher C. Joyner and Catherine Lotrionte, "Information Warfare as International Coercion: Elements of a Legal Framework", EJIL, Vol 12, #5, 825-865, 2001

8. Col Kenneth Allard, "*Information Operations in Bosnia: A Preliminary Assessment*", NDU Strategic Forum, #91, Nov 1996

9. Colonels Qiao Liang and Wang Xiangsui, "*Unrestricted Warfare*", Beijing: PLA Literature and Arts Publishing House, Feb 1999

10. Department of Defense Paper, "*Assessment of International Legal Issues in Information Operations*", Nov 1999

11. Dr. Dan Kuehl, "*Joint Information Warfare: An Information-Age Paradigm for Jointness*", NDU Strategic Forum, #105, Mar 1997

12. Edward Donald Kennedy, "King Arthur – A Casebook", Routledge Publishers (Great Britain), 2002

13. Field Manuel 100-06, *Army Information Operations, 17 Aug 1996*

14. From LTC(P) Ronald M. Bouchard, "*Information Operations in Iraq*", Strategy Research Project, U.S. Army War College, 1999

15. Gary Hamel and C.K. Prahalad, "Competing for the Future", Harvard Business School Press (1994)

16. Gen John M. Shalikashvili, Former Chairman, Joint Chiefs of Staff, "National Military Strategy", 1998

17. George S. Day / David J. Reibstein, "Wharton on Dynamic Competitive Strategy", John Wiley & Sons, Inc. (1997)

18. Jeffery A. Krames, "*The Rumesfeld Way: The Leadership Wisdom of a Battle-hardened Maverick*", McGraw Hill Press, Mar 2002

19. Joint Publication 3-13, "*Joint Information Operations*"

20. Joint Publication 3-61, "Public Affairs in Joint Operations"

21. Joint Vision 2010, http://www.dtic.mil/jv2020/

22. Kenneth Allard, "*Information Operations in Bosnia, A Preliminary Assessment*", National Defense University Strategic Forum, #91, Nov 1998

23. Liam Fahey / Robert M. Randall, "The Portable MBA in Strategy", John Wiley & Sons, Inc (2001)

24. Lieutenant Colonel Henry Huntly, Maj Michael Yaguchi, and Lieutenant Commander Michael Goshgarian, "*Another Battlefield Domain? How the Media Impacts Joint Operations*", JFSC Paper, Sep 2000

25. LT CDR William J. Jensen, "*Information Warfare's Missing Quarterback – The Case for a Joint Force Information Warfare Component Commander*", Naval War College, Feb 1998

26. Lt Col (P) Wendell B. McKeown, *Information Operations: Countering the Asymmetric Threat to the United States*, Air War College, Jun 1999

27. Lt Col Blake F. Lindner, "*Information Operations: America's Plan for Strategic Failure*", Air War College, Apr 1998

28. Lt Col David Wolfe, *Information Management* (PowerPoint), JCIWS/JC4ISOC, May 2002

29. Lt Col Tom Jukes, "*Battlespace Management - Campaigning Strategy*" (PowerPoint), Joint Forces Staff College / NDU, 2002

30. Maj Dennis J. DiCenso, "*IW Cyberlaw-The Legal Issues of Information Warfare*", Aerospace Power Journal, Summer 1999

31. Maj Gary Pounder, "*Opportunity Lost – Public Affairs, Information Operations and the War Against Serbia*", Aerospace Power Journal, Summer 2000

32. Maj Seshagiri Munipalli, "*Information Operations: Moving from Doctrine to Execution*", Air Command and Staff College, April 1999

33. Martin C. Libicki, "*Information Dominance*", NDU Strategic Forum, #132, Nov 1997

34. Michael Porter, "Competitive Advantage - Creating and Sustaining Superior Performance", The Free Press (1985) [Differentiation and the Technology Value Chain Model, and Achieving Relationships]

35. Michael Porter, "Competitive Strategy - Techniques for Analyzing Industries and Competitors", The Free Press (1980)

36. National Security Strategy, 1997, http://clinton2.nara.gov/WH/EOP/NSC/Strategy/

37. Naval Doctrine Publication 6: Naval Command and Control, Department of the Navy, May 1995

38. PDD 63, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

39. Ralf Beadrath, "*The Cyberwar Debate: Perception and Politics in U.S. Critical Infrastructure Protection*", Information and Security, Vol 7 (2001)

40. Randall C. Lane, "*Information Operations: A Joint Perspective*", Army School of Advanced Military Studies, 21 may 1998

41. Sun Tzu, "The Art of War"

42. Testimony of James Adams, CEO, Infrastructure Defense Inc., Committee on Governmental Affairs, U.S. Senate, Mar 2000

43. Thomas Baines, "*Military Information Operations: An Unifying Paradigm*", A Paper for the Center of Defense Information